Testimony before the U.S. House Subcommittee on Election Security and Integrity

Steven S. Sandvoss

Executive Director

Illinois State Board of Elections

As the Committee is aware, in June of 2016 the Illinois State Board of Elections (SBE) was the victim of a cyber-attack which at the time was of unknown origin. It has since been learned that the attack was perpetrated by Russian operatives who were seeking unauthorized access into the voter registration database maintained by the SBE. In response to this attack, measures were immediately undertaken to close the access point of the intrusion, assess the extent of the penetration, determine whether any data was manipulated or destroyed, and ascertain which voter records were improperly accessed, with the purpose of alerting said voters and giving guidance to assist them in protecting their sensitive information. It should be noted that an analysis of the breach did not reveal any evidence that specific voters were targeted or that the attack focused on any particular region or demographic. The SBE quickly alerted Federal law enforcement, and fully cooperated with their investigation. Following the initial steps described above, the SBE undertook an unprecedented effort to secure its voter registration database as well as other IT related applications.

In March of 2018, the EAC provided $380 million in grant money to the states to assist in their cyber-security efforts. Illinois' share was $13.2 million, with a requirement that the State provide a 5% match; which amounted to $661,615. Shortly after receiving this grant money,

legislation was passed in Illinois that earmarked no less than half of the grant money to a Cyber-Navigator Program (CNP), to be created and administered by the SBE.

In order to receive any of the grant money, Illinois' Election Authorities (EAs) must agree to participate in the CNP. (The EAs consist of 101 county clerks, 1 county board of election commissioners and 6 city boards of election commissioners, who are responsible for maintaining a list of registered voters within their jurisdiction, securing election voting and tabulating equipment and conducting the actual election on election day, as well as early and mail in voting.)

The CNP consists of 3 basic parts; 1) Requiring the EAs to adopt the Illinois Century Network (ICN) as their internet service provider for all traffic between their offices and the SBE. 2) Engaging in a Cyber Security Information Sharing Program with the EAs to share cyber-security related information and 3) Creation of a team of "Cyber Navigators" to provide cyber-assistance to the EAs.

Illinois Century Network (ICN)

The ICN is a state managed network delivering network and internet services to government agencies in Illinois. The goal of the ICN is to provide EAs with a cleaner and safer internet. The SBE Plan would bring all network traffic to and from the EAs to an internal "10 dot IP" network system and "whitelisting" IP addresses for access to the IVRS website. Isolating this network to one under the complete control of the SBE and Department of Innovation and Technology (DoIT) ensures that voter registration data and EA management operations never actually flow

over the internet. Additionally, this provides us the ability to provide additional security measures and monitoring.

Cyber Security Information Sharing Program-

In partnership with the Illinois State Police's division of Statewide Terrorism and Intelligence Center (STIC), the SBE is overseeing the Cyber Security Information Sharing Program, which involves researching and gathering of information related to pertinent cyber-attacks and cyber resiliency and sharing that information with all federal and state stakeholders. Our goal is to consolidate numerous information sources and, with feedback from local Election Authorities, distill it into the most valuable, actionable information possible.

Cyber Navigators

The Cyber Navigators are assisting the EAs by performing onsite risk assessments and providing resources to ensure Election Security for 2020 and beyond. Currently 9 Navigators are assigned in 4 regional zones in the state. (2 per zone, and 1 lead navigator). The Navigators will be offering additional services such as phishing assessments, penetration testing and educational trainings. They will also be performing additional risk assessments on physical security and best practices in securing voting equipment.

In addition to the CNP, the SBE worked in partnership with the Illinois National Guard's cyber security team to coordinate a cyber-defense system to provide cyber protection for both the SBE and the EAs prior to and on Election Day. Members of the Guard were stationed in all regions of

the state, at the SBE, at STIC and their own bases to be ready in the event of a statewide cyber event.

Following the creation of the CNP, the SBE released $2.9 million of the aforementioned grant funds to the participating EAs to make purchases to upgrade election related computer systems and to address cyber vulnerabilities identified through scans, Cyber Navigators or other assessments of existing election systems. Funds could also be used to implement cyber security best practices for election systems and other activities designed to improve the security of the election systems.

In addition to the CNP, the SBE took the following steps to beef up its own cyber security.

Investments in Personnel

- Hired two additional highly experienced IT staff, including a Security Analyst with 20 years of Information Security experience

Investments in Hardware

- Purchased Web Application Firewalls to protect against attacks on the SBE's public-facing applications
- Purchased new firewalls with Intrusion Prevention Systems

Investments in Software

- Implemented "Next-Generation" Endpoint Protection products to protect SBE computers and servers from the latest types of ransomware, Trojans, and other types of malware.

"Next-Generation" implies that the products protect against the *behavior* of malware rather than simply blocking it based on definition

- Implemented endpoint server protection products to detect and prevent attacks against the SBE's web applications and sites
- Implemented a new Web Security Gateway to provide filtering and protection against malicious links and to monitor traffic for signs of compromise

Security Assessments

- Completed the Department of Homeland Security's "Risk & Vulnerability Assessment" in early 2018
- Deployed our own vulnerability scanning solution to allow us to perform regular, internal scans of our environment for vulnerabilities at a deeper level possible than from external scans
- Completed a penetration test in partnership with the Department of Innovation & Technology's Information Security staff before the 2018 mid-term election

Ongoing Monitoring

- The SBE's IT entire environment is monitored by the Department of Innovation & Technology's Security Operations Center
- All SBE network traffic now flows through an Albert sensor provided by the Department of Innovation and Technology

Looking to the future, the SBE believes it is necessary to maintain the Cyber Navigator Program indefinitely and possibly expand it to address the continuing needs of the EAs. Cyber Security is an ongoing, ever escalating process that doesn't have an end date, and as such there will be an

ongoing need for funds to maintain the program. At present, the primary mission of the Cyber-Navigators is to perform risk assessments of the IT systems of all the EAs who are participating in the CNP (currently there are 90 EAs participating and 81 risk assessments have been scheduled or performed). Once these assessments are completed, the SBE will be in a position to better understand what types of systems will need to be created and what upgrades will be needed to improve existing systems within each EAs jurisdiction which can be done through the purchases made and reimbursed through the grant requests. Since the risk assessments are ongoing, it is not possible to give a cost estimate to implement said systems and upgrades at this time.

Lastly, the EA community has repeatedly stated to the SBE that their primary need with respect to ensuring the integrity of their elections is the replacement of the voting systems within their jurisdictions, many of which are almost 20 years old. In terms of technology, said systems are ancient and need to be replaced. The SBE anticipates needing approximately $175 million to replace the systems that are currently in use in Illinois (There are approximately 25,000 voting system components in Illinois consisting of Optical Scan, Direct Recording Electronic machines (DRE or what is commonly referred to as touchscreen voting) and Ballot Marking Devices. This estimate is based on the State of Ohio's recent solicitation of new voting equipment, in which some of the bidding vendors also do business in Illinois and presumably their quotes would be the same. This estimate however does not factor in additional costs that would likely result once the new 2015 Voluntary Voting System Guidelines version 2.0 are approved by the EAC (Illinois is expected to adopt those standards). Said Guidelines will recommend additional security features that would better protect the voting systems from cyber-attack as well as

provide increased accessibility for voters with disabilities. Unfortunately, it is not possible at this point to provide an accurate prediction of what the costs would be of said systems and it is also unknown as to when the vendors will have these systems available for use in Illinois, as they have to go through a rather lengthy testing and certification process.

Thank you for your consideration.